

IN THE SPECIFICATION:

In accordance with 37 CFR 1.125 (b)(2) please amend the specification as set forth in a Substitute Specification, as attached. Additionally, in accordance with 37 CFR 1.125(c), a marked-up version of the Substitute Specification is also attached.

#5
(D.E.)
6-20-03
[Signature]

FINGERPRINT COLLATING DEVICE AND FINGERPRINT COLLATING METHOD

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to a fingerprint collating device and a fingerprint collating method, and more particularly, is suitably applied to a fingerprint collating device to effect personal authentication by using the fingerprint, for example.

DESCRIPTION OF THE RELATED ART

Conventionally, there is a fingerprint collating unit for effecting personal authentication by using the fingerprint. Such fingerprint collating unit uses an image pick-up element to photograph a user's fingerprint, and produce a fingerprint image. And the fingerprint collating unit collates the photographed fingerprint image with the registered fingerprint image for collation to effect personal authentication. The fingerprint is unchanged throughout one's life and different from person to person. Therefore, the fingerprint can securely assure the personal authentication.

However, the third party may pick up the other's fingerprint from a cup or the like, for example, to falsify a fingerprint image, and enter the falsified fingerprint image into the fingerprint collating unit for the fingerprint collation. The third party may abuse the falsified fingerprint for personal authentication.

*please
enter
RTM*

SUMMARY OF THE INVENTION

In view of the foregoing, an object of this invention is to provide a fingerprint collating device and a fingerprint collating method which can prevent an illicit use of the other's fingerprint.

The foregoing object and other objects of the invention have been achieved by the provision of a fingerprint collating device for collating a user's fingerprint the registered fingerprint information to effect personal authentication, comprising fingerprint reader for reading the user's fingerprint to create read fingerprint information, and to create read history information indicating that the read fingerprint information has been created, read history storage for storing the read history information, and collator for collating the read fingerprint information with the registered fingerprint information to effect personal authentication and output a result of authentication when the read history information is stored in the read history storage.

The read history information indicating that the read fingerprint information has been created is stored in the read history storage, and the read fingerprint information is collated with the registered fingerprint information to effect personal authentication when the read history information is stored in the read history storage. Therefore, even if the read fingerprint information is improperly entered from the outside, the personal authentication is not effected, leading to prevention of an illicit use.

The nature, principle and utility of the invention will become more apparent from the following detailed description when read in conjunction with the accompanying drawings in which like parts are designated by like reference numerals or characters.

BRIEF DESCRIPTION OF THE DRAWINGS

In the accompanying drawings:

Fig. 1 is a block diagram showing the configuration of a fingerprint collation system according to the present invention;

Fig. 2 is a block diagram showing the configuration of a fingerprint collating unit; and

Fig. 3 is a diagram showing a stored state of fingerprint data.

DETAILED DESCRIPTION OF THE EMBODIMENT

Preferred embodiments of this invention will be described with reference to the accompanying drawings:

(1) Overall Configuration of a Fingerprint Collation System

In Fig. 1, reference numeral 1 denotes a fingerprint collation system of the invention as a whole, in which a card reader 20 for reading or writing data from or to an Integrated Circuit (IC) card 21 and a fingerprint collating unit 30 as a fingerprint collating device are connected to a personal computer 10. The personal computer 10 is connected to the card reader 20, as well as the fingerprint collating unit 30, via an RS-232C serial interface.

The fingerprint collating unit 30 accepts a user's fingerprint, and collates the fingerprint with either a fingerprint template (reference fingerprint data for the person for authentication) registered in the fingerprint collating unit 30 or a fingerprint template registered in the IC card 21, a result of fingerprint collation being output to the personal computer 10.

The fingerprint collating unit 30 has a plurality of fingerprint templates registered, each fingerprint template being identified by an index number N index. Also, the IC card 21 has a fingerprint template of an owner of the IC card 21 registered.

(2) Fingerprint Registration Process

When the fingerprint of a person for authentication is registered in the fingerprint collating unit 30, the personal computer 10 sends a fingerprint registration instruction Reg and an index number N index specified by the user to the fingerprint collating unit 30 in response to the fingerprint registration operation of the user.

Fig. 2 is a diagram of the fingerprint collating unit 30 as a whole. A CPU 31, a program Random Access Memory (RAM) 32, a program flash Read Only Memory (ROM) 33, and a collation controller 34 are connected to a main bus 39. The CPU 31 reads a control program from the program flash ROM 33 and executes the control program in the program RAM 32 to control the whole of the fingerprint collating unit 30.

That is, the CPU 31 receives the fingerprint registration instruction Reg and the index number N index sent from the personal computer 10 via a RS232C driver 38. And the CPU 31 controls the collation controller 34 in accordance with the fingerprint registration instruction Reg to start reading the fingerprint.

The collation controller 34 turns on an LED 41 under the control of the CPU 31 to apply an illuminating light L1 onto the bottom face of a prism 50. Then, the user puts one's finger with fingerprint face to be registered on the slant of the prism 50 firmly.

The prism 50 reflects the illuminating light L1 on the interior of the slant of prism to cause a reflected light L2 to be outgoing via a lens (not shown) provided within a lens barrel 51

to a Charge Coupled Device (CCD) 40. The prism 50 reflects totally the illuminating light L1, when there is an air layer on the outer face of the slant, while diffusing the illuminating light L1, when there is no air layer on the outer face of the slant. Therefore, when the user puts one's finger with fingerprint face firmly on the slant of the prism 50, the illuminating light L1 is reflected at a concave portion of the fingerprint due to the presence of air layer, while being diffused at a convex portion of the fingerprint due to the absence of air layer. Consequently, the reflected light L2 results in an image which is bright in the concave portion of fingerprint and dark in the convex portion of fingerprint. The CCD 40 produces an image signal S40 by picking up the reflected light L2, and outputs the image signal S40 to an analog/digital converter 37. In this way, the fingerprint is optically read.

The analog/digital converter 37 converts the image signal S40 into a digital signal, which is binarized and output as the fingerprint image data D37 to the collation controller 34. At this time, the collation controller 34 displays the fingerprint image data D37 via the RS232C driver 38 on a monitor 11 of the personal computer 10 (Fig. 1). Thereby, the user confirms one's own fingerprint photographed to adjust the disposition of the finger with respect to the prism 50.

The collation controller 34 extracts the feature points of fingerprint (central or branch point of fingerprint pattern) from the fingerprint image data D37 to produce a fingerprint template Temp. And the collation controller 34 registers the fingerprint template Temp and an attribute Attb associated with the fingerprint template Temp at an index (address) specified by the index number N index within the collation flash ROM 35, as shown in Fig. 3, and notifies the personal computer 10 that the registration of fingerprint has been completed (Fig. 1).

(3) Fingerprint Collation Process

(3-1) Fingerprint collation process with fingerprint template within fingerprint collating unit

When the fingerprint collation is performed by using a fingerprint template Temp registered within the fingerprint collating unit 30, the user uses the personal computer 10 to start a fingerprint collation process and input an index number N index. The personal computer 10 sends a fingerprint collation instruction Ref and the index number N index specified by the user to the fingerprint collating unit 30 in response to this.

In Fig. 2, the CPU 31 receives the fingerprint collation instruction Ref and the index number N index sent from the personal computer 10 via the RS232C driver 38, controls the collation controller 34 in accordance with the fingerprint collation instruction Ref to start reading the fingerprint.

The collation controller 34 turns on the LED 41 under the control of the CPU 31, like when registering the fingerprint, and applies an illuminating light L1 on the bottom face of the prism 50. At this time, the user puts one's finger with fingerprint face on the slant of the prism 50 firmly.

The prism 50 reflects the illuminating light L1 at the interior of the slant of prism, and causes the reflected light L2 representing the user's fingerprint image to be outgoing via a lens (not shown) provided within the lens barrel 51 to the CCD 40 which is fingerprint reading means. The CCD 40 picks up the reflected light L2 to produce an image signal S40 for output to the analog/digital converter 37. The analog/digital converter 37 converts the image signal S40 into a digital signal, which is binarized and output as the fingerprint image data D37 to the collation controller 34.

Here, when the fingerprint image data D37 is normally produced, the collation controller 34 which is fingerprint reading means sets a fingerprint accepting flag as reading history

information indicating that the fingerprint has been read in the program RAM 32 which is reading history storing means.

And the collation controller 34 as collating means reads the fingerprint template Temp specified by the index number N index from the collation flash ROM 35 and collates the fingerprint image data D37 with the read fingerprint template Temp.

At this time, the collation controller 34 executes the collation between the fingerprint template Temp and the fingerprint image data D37, only when the fingerprint accepting flag has been set in the program RAM 32, but does not execute the collation when the fingerprint accepting flag has not been set in the program RAM 32. Namely, the fingerprint collating unit 30 performs the collation of fingerprint only with the fingerprint image data D37 read by the fingerprint collating unit 30, but does not perform the collation of fingerprint even if the fingerprint image data D37 is input externally. Thereby, it is possible to prevent an illicit use of fingerprint, using the falsified fingerprint image data.

After the collation between the fingerprint template Temp and the fingerprint image data D37 has been completed, the collation controller 34 resets the fingerprint accepting flag in the program RAM 32, and outputs a result of collation to the personal computer 10 (Fig. 1).

(3-2) Fingerprint collation process with fingerprint template within IC card

When the collation of fingerprint is made using the fingerprint template Temp registered within the IC card 21, the user inserts the IC card 21 into the card reader 20, and uses the personal computer 10 to start the fingerprint collation operation. The personal computer 10 sends a fingerprint collation instruction Ref to the fingerprint collating unit 30 in response to this.

The CPU 31 (Fig. 2) controls the collation controller 34 in accordance with the fingerprint collation instruction Ref to start reading the fingerprint. The collation controller 34 reads a user's fingerprint to produce the fingerprint image data D37 and store it in the collation RAM 36 under the control of the CPU 31, like when registering the fingerprint. Herein, when the fingerprint image data D37 can be normally produced, the collation controller 34 sets the fingerprint accepting flag indicating that the fingerprint has been read in the program RAM 32.

The collation controller 34 reads the fingerprint template Temp registered within the IC card 21 via the personal computer 10, and stores the fingerprint template Temp at an index #0 in the collation flash ROM 35. And the collation controller 34 reads the fingerprint template Temp from the index #0 in the collation flash ROM 35, and performs the collation between the fingerprint template Temp and the fingerprint image data D37.

At this time, the collation controller 34 executes the collation between the fingerprint template Temp and the fingerprint image data D37, only when the fingerprint accepting flag has been set in the program RAM 32, but does not execute the collation when the fingerprint accepting flag has not been set in the program RAM 32.

After the collation between the fingerprint template Temp and the fingerprint image data D37 has been completed, the collation controller 34 resets the fingerprint accepting flag in the program RAM 32, and outputs a result of collation to the personal computer 10 (Fig. 1).

(4) Operation and Effect

In the above configuration, the fingerprint collating unit 30 accepts a user's fingerprint to produce the fingerprint image data D37. At this time, when the fingerprint image data D37 is

normally produced, the collation controller 34 sets the fingerprint accepting flag in the program RAM 32.

And the collation controller 34 performs the collation between the fingerprint template Temp within the fingerprint collating unit 30 or the IC card 21 and the fingerprint image data D37, only when the fingerprint accepting flag has been set in the program RAM 32.

With the above configuration, the fingerprint accepting flag is set when the user's fingerprint is accepted to produce the fingerprint image data D37. Only when the fingerprint accepting flag has been set, the collation of fingerprint is performed. Therefore, even if the fingerprint image data D37 is entered externally into the fingerprint collating unit 30, the collation of fingerprint is not performed. Consequently, it is possible to prevent an illicit use of fingerprint, using the falsified fingerprint image data.

As described above, according to the present invention, the read history information representing that the read fingerprint information has been produced is stored in the read history storing means. When the read history information is stored in the read history storing means, the collation between the read fingerprint information and the registered fingerprint information is performed to effect personal authentication. Even if the read fingerprint information is entered externally and illicitly, the personal authentication is not performed. Consequently, it is possible to provide the fingerprint collating device which can prevent an illicit use of fingerprint.

While there has been described in connection with the preferred embodiments of the invention, it will be obvious to those skilled in the art that various changes and modifications may be aimed, therefore, to cover in the appended claims all such changes and modifications as fall within the true spirit and scope of the invention.